Отчёт по лабораторной работе 16

Базовая защита от атак типа «brute force»

Авдадаев Джамал Геланиевич

Содержание

Список иллюстраций

Список таблиц

1 Введение

1.1 Цель работы

Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

2 Процесс работы

2.1 Установка и запуск Fail2ban

2.1.1 Установка Fail2ban

На сервер был установлен пакет `fail2ban` с помощью менеджера пакетов DNF. После завершения установки система вывела сообщение о том, что все необходимые компоненты были успешно добавлены.

Рис. 2.1: Установка и запуск fail2ban

Сервис Fail2ban был запущен и включён в автозагрузку.
Система создала символьную ссылку в директории `multi-user.target.wants`, подтверждающую успешную активацию сервиса.

2.1.2 Просмотр журнала Fail2ban

Для проверки работы Fail2ban был открыт журнал событий.
Записи в логе показывают:

- запуск серверной части Fail2ban;

- запуск наблюдателя;
- подключение к базе данных;
- создание новой базы при первом запуске.

```
[dgavdadaev@server.dgavdadaev.net ~]$
[dgavdadaev@server.dgavdadaev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for dgavdadaev:
2025-12-11 11:15:41,470 fail2ban.server         [17953]: INFO    --------------------------------------------------
2025-12-11 11:15:41,470 fail2ban.server         [17953]: INFO    Starting Fail2ban v1.1.0
2025-12-11 11:15:41,470 fail2ban.observer       [17953]: INFO    Observer start...
2025-12-11 11:15:41,474 fail2ban.database       [17953]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sq
lite3'
2025-12-11 11:15:41,474 fail2ban.database       [17953]: WARNING New database created. Version '4'
```

Рис. 2.2: Просмотр журнала Fail2ban

2.1.3 Создание локального файла конфигурации и включение защиты SSH

Для хранения индивидуальных настроек создан файл в `jail.d`.
В него добавлены параметры блокировки и включена защита SSH, включая несколько jail-ов для разных типов атак.

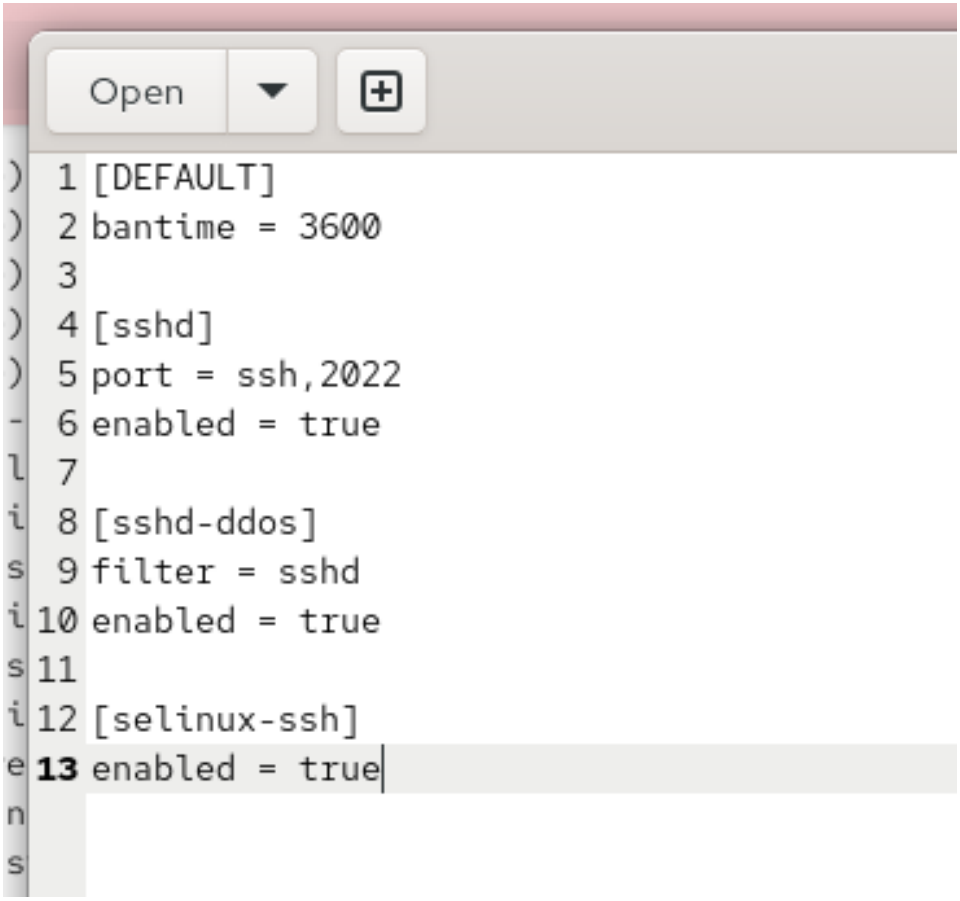

Рис. 2.3: Локальная конфигурация Fail2ban SSH

После перезапуска Fail2ban в журнале появились записи о создании и запуске jail-ов:

- `sshd`;
- `selinux-ssh`;
- `sshd-ddos`.

Все jail-ы корректно активировались и начали обработку данных журналов.

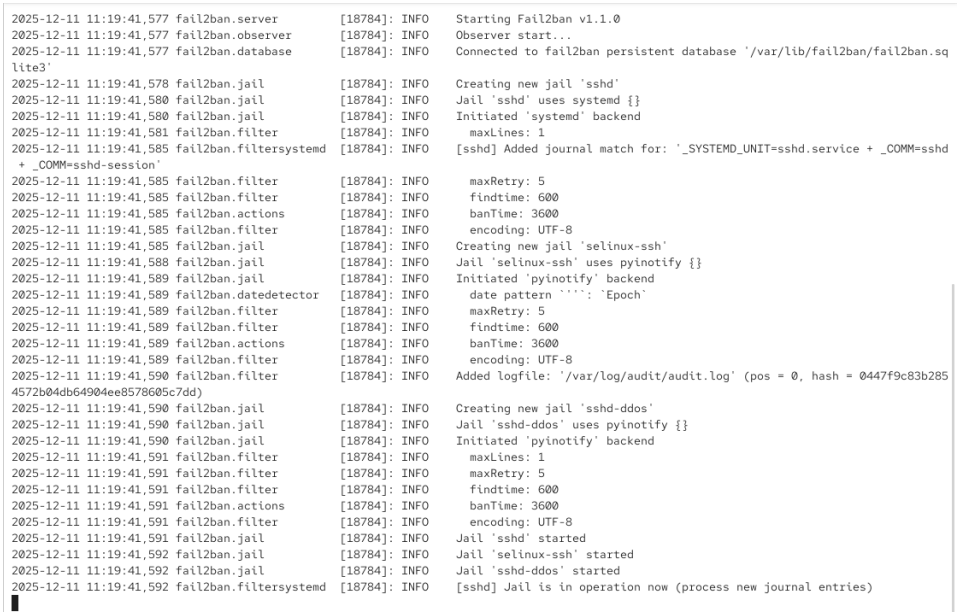

Рис. 2.4: Создание и запуск jail-ов SSH

2.1.4 Включение защиты HTTP-сервисов

В локальный файл конфигурации были добавлены HTTP-jail-ы для защиты Apache от различных типов атак.

Рис. 2.5: Включение HTTP-jail-ов

После перезапуска Fail2ban журнал показал инициализацию каждого HTTP-jail-а, добавление их лог-файлов и успешный запуск.

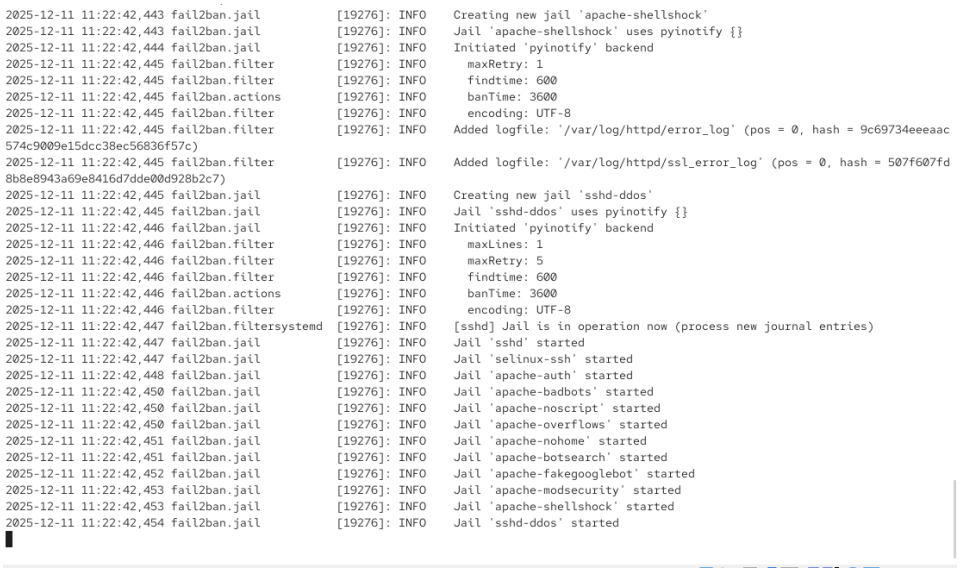

Рис. 2.6: Работа HTTP-jail-ов

2.1.5 Включение защиты почтовых сервисов

В локальной конфигурации были включены jail-ы для защиты почтовых сервисов: Postfix, Dovecot и других.

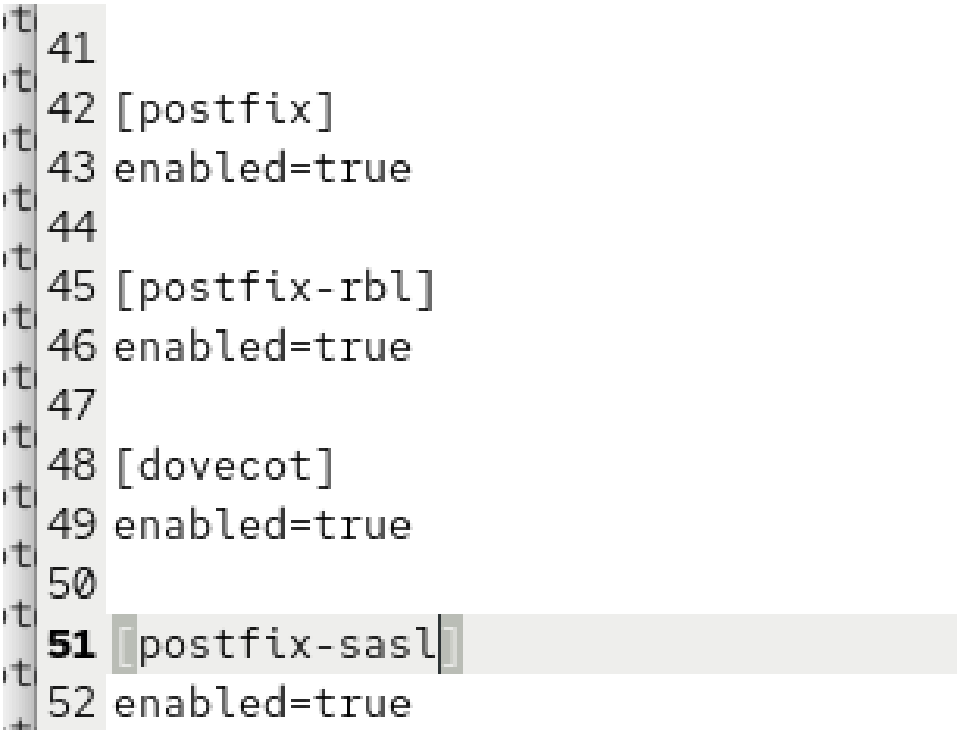

Рис. 2.7: Включение защиты почтовых сервисов

После очередного перезапуска Fail2ban были созданы и запущены дополнительные jail-ы, что видно в логе:

- защита Postfix;
- защита SASL;
- защита Dovecot;
- активация RBL-фильтрации.

```
SYSTEMD_UNIT=postfix@-.service
2025-12-11 11:24:36,669 fail2ban.filter         [19613]: INFO      maxRetry: 5
2025-12-11 11:24:36,669 fail2ban.filter         [19613]: INFO      findtime: 600
2025-12-11 11:24:36,669 fail2ban.actions        [19613]: INFO      banTime: 3600
2025-12-11 11:24:36,669 fail2ban.filter         [19613]: INFO      encoding: UTF-8
2025-12-11 11:24:36,669 fail2ban.jail           [19613]: INFO    Creating new jail 'sshd-ddos'
2025-12-11 11:24:36,669 fail2ban.jail           [19613]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:24:36,670 fail2ban.jail           [19613]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      maxLines: 1
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      maxRetry: 5
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      findtime: 600
2025-12-11 11:24:36,670 fail2ban.actions        [19613]: INFO      banTime: 3600
2025-12-11 11:24:36,670 fail2ban.filter         [19613]: INFO      encoding: UTF-8
2025-12-11 11:24:36,671 fail2ban.filtersystemd  [19613]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,671 fail2ban.jail           [19613]: INFO    Jail 'sshd' started
2025-12-11 11:24:36,671 fail2ban.jail           [19613]: INFO    Jail 'selinux-ssh' started
2025-12-11 11:24:36,672 fail2ban.jail           [19613]: INFO    Jail 'apache-auth' started
2025-12-11 11:24:36,672 fail2ban.jail           [19613]: INFO    Jail 'apache-badbots' started
2025-12-11 11:24:36,672 fail2ban.jail           [19613]: INFO    Jail 'apache-noscript' started
2025-12-11 11:24:36,673 fail2ban.jail           [19613]: INFO    Jail 'apache-overflows' started
2025-12-11 11:24:36,673 fail2ban.jail           [19613]: INFO    Jail 'apache-nohome' started
2025-12-11 11:24:36,673 fail2ban.jail           [19613]: INFO    Jail 'apache-botsearch' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'apache-fakegooglebot' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'apache-modsecurity' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'apache-shellshock' started
2025-12-11 11:24:36,674 fail2ban.jail           [19613]: INFO    Jail 'postfix' started
2025-12-11 11:24:36,675 fail2ban.filtersystemd  [19613]: INFO    [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,675 fail2ban.filtersystemd  [19613]: INFO    [postfix] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,675 fail2ban.jail           [19613]: INFO    Jail 'postfix-rbl' started
2025-12-11 11:24:36,676 fail2ban.jail           [19613]: INFO    Jail 'dovecot' started
2025-12-11 11:24:36,676 fail2ban.filtersystemd  [19613]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,676 fail2ban.jail           [19613]: INFO    Jail 'postfix-sasl' started
2025-12-11 11:24:36,676 fail2ban.filtersystemd  [19613]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,676 fail2ban.jail           [19613]: INFO    Jail 'sshd-ddos' started
```

Рис. 2.8: Работа почтовых jail-ов

2.2 Проверка работы Fail2ban

Для проверки работоспособности Fail2ban был просмотрен общий статус сервиса.

В выводе отображается количество активных jail-ов и их список.

```
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript,
apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.dgavdadaev.net server]# fail2ban-client set sshd maxretry 2
2
[root@server.dgavdadaev.net server]#
```

Рис. 2.9: Общий статус Fail2ban

Был просмотрен статус jail-а `sshd`, где отображаются:

- количество неудачных попыток входа;
- количество заблокированных IP-адресов;

- список заблокированных адресов.

```
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.dgavdadaev.net server]#
```

Рис. 2.10: Статус защиты SSH

Для усиления защиты была установлена величина максимального количества ошибок при попытке входа:

```
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript,
apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.dgavdadaev.net server]# fail2ban-client set sshd maxretry 2
2
[root@server.dgavdadaev.net server]#
```

Рис. 2.11: Установка maxretry

После нескольких неудачных попыток входа с клиента Fail2ban заблокировал адрес, что подтверждается обновлённым статусом jail-а.

```
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.dgavdadaev.net server]#
```

Рис. 2.12: Блокировка IP после неудачных попыток входа

IP-адрес клиента был успешно разблокирован с помощью соответствующей команды.

После выполнения команды статус jail-а обновился, и количество текущих блокировок стало равно нулю.

```
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.dgavdadaev.net server]#
```

Рис. 2.13: Разблокировка адреса клиента

В локальную конфигурацию Fail2ban было добавлено исключение, запрещающее блокировать определённый IP-адрес.
Изменение внесено в раздел `[DEFAULT]` файла локальной конфигурации.

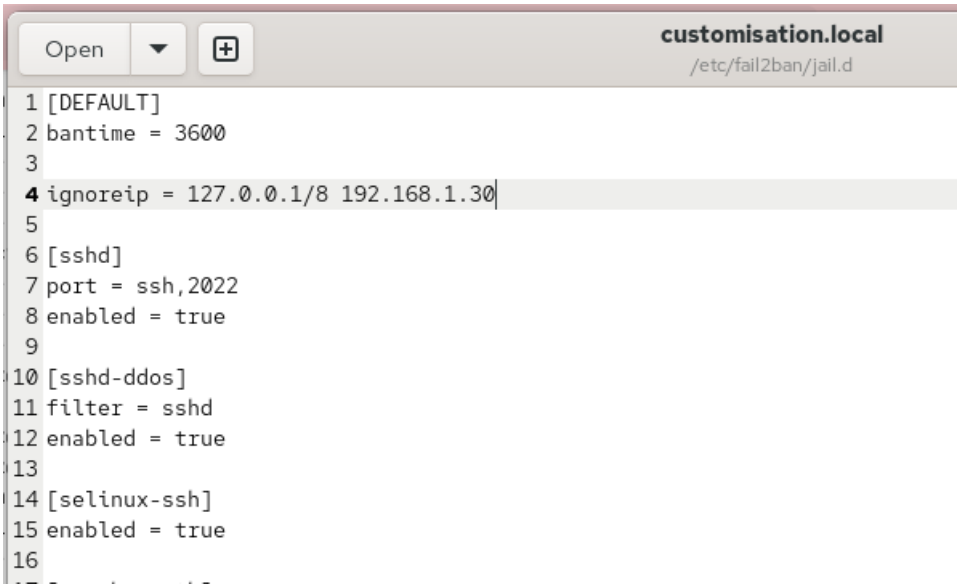

Рис. 2.14: Добавление ignoreip

После перезапуска Fail2ban в журнале появилось подтверждение, что указанный IP теперь игнорируется.

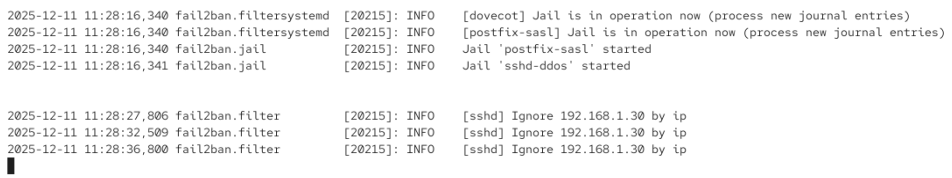

Рис. 2.15: Fail2ban игнорирует IP-адрес клиента

После внесения IP в `ignoreip` повторная попытка входа с неправильным паролем не привела к блокировке, что подтверждается отсутствием записей о бане в статусе jail-a `sshd`.

2.3 Внесение изменений во внутреннее окружение виртуальной машины

На виртуальной машине были созданы каталоги для хранения кастомных конфигураций Fail2ban, которые используются при provisioning'е Vagrant.

```
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# cd /vagrant/provision/server/
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.dgavdadaev.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d
/
[root@server.dgavdadaev.net server]# touch protect.sh
[root@server.dgavdadaev.net server]#
```

Рис. 2.16: Создание каталогов и копирование конфигурации

В каталоге `/vagrant/provision/server` был создан исполняемый файл `protect.sh`, содержащий:

- установку Fail2ban;
- копирование заранее подготовленных конфигураций;
- восстановление контекстов SELinux;
- запуск и включение Fail2ban в автозагрузку.

Vagrantfile | netlog.sh | netlog.sh | protect.sh

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install fail2ban
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/protect/etc/* /etc
7  restorecon -vR /etc
8  echo "Start fail2ban service"
9  systemctl enable fail2ban
10 systemctl start fail2ban
```

Рис. 2.17: Скрипт protect.sh

3 Итоги

3.1 Вывод

Fail2ban обеспечивает автоматическую защиту сервера, анализируя журналы и блокируя источники подозрительной активности. В ходе работы были настроены jail-ы для SSH, веб- и почтовых служб, проверена блокировка и разблокировка IP, добавлены исключения, а также подготовлен provisioning-скрипт для автоматизации конфигурации. Система функционирует корректно и эффективно повышает безопасность сервера.

3.2 Контрольные вопросы

1. Поясните принцип работы Fail2ban. Fail2ban анализирует журналы системных сервисов и отслеживает повторяющиеся ошибки (например, неудачные попытки входа). При превышении установленного лимита программа динамически добавляет правила в брандмауэр и блокирует IP-адрес нарушителя на заданное время.

2. Настройки какого файла более приоритетны: jail.conf или jail.local? Наиболее приоритетны настройки **jail.local** — именно этот файл предназначен для переопределения значений по умолчанию, указанных в *jail.conf*.

3. Как настроить оповещение администратора при срабатывании Fail2ban? В секции действий Fail2ban можно указать отправку email-сообщений. Для этого выбирают action, поддерживающий уведомления, например:

- `action = %(action_mwl)s`

Также необходимо корректно настроить локальную почтовую систему, чтобы Fail2ban мог отправлять письма.

4. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к веб-службе. Основные параметры для веб-служб включают:

- указание соответствующих фильтров для Apache/Nginx;
- выбор лог-файлов, которые должны анализироваться;
- активацию или деактивацию нужных jail-ов;
- настройку временных интервалов (findtime, bantime);
- определение лимита ошибок (maxretry).

Эти параметры задают общие правила мониторинга веб-сервера и его реакцию на подозрительные запросы.

5. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к почтовой службе. Стандартные секции для почтовых служб включают:

- выбор фильтра (например, postfix, dovecot);
- включение или отключение конкретного jail-а;
- указание логов почтовых сервисов;
- определение временных интервалов и числа попыток;
- выбор действий при обнаружении попыток взлома.

Эти настройки позволяют контролировать работу SMTP/IMAP/POP сервисов и блокировать попытки подбора паролей.

6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где посмотреть описание действий? Fail2ban может:

- блокировать IP через firewall;

- отправлять уведомления администратору;
- выполнять пользовательские скрипты;
- объединять несколько действий в один сценарий.

Описание действий находится в директории:

- `/etc/fail2ban/action.d/`

Каждый файл описывает конкретное действие и может использоваться в настройках jail-ов.

7. Как получить список действующих правил Fail2ban? Получить список активных jail-ов можно с помощью:

- `fail2ban-client status`

Этот вывод включает общее количество jail-ов и их названия.

8. Как получить статистику заблокированных Fail2ban адресов? Используют команду:

- `fail2ban-client status <jail>`

Она показывает:

- число текущих блокировок;
- общее количество заблокированных IP;
- список заблокированных адресов.

9. Как разблокировать IP-адрес? Для снятия блокировки выполняется команда:

- `fail2ban-client set <jail> unbanip <IP>`

Она удаляет IP из списка заблокированных и снимает правило из брандмауэра.